ABSTRACT

There is provided a system for detecting and tracing a (D)DoS attack and identifying the attack source, which system simplifies the judgment reference to determine whether a (D)DoS attack is present. The number of source addresses of the pockets transmitted via the Internet line is monitored. When the number of the source addresses has reached a predetermined number or a predetermined ratio within a predetermined time, it is judged that an unauthorized attack is present. Moreover, the packet of the HOP number different from the HOP number corresponding to the transmission source information is judged to be unauthorized information.